REMARKS

Reconsideration of this application is requested. Claims 9-16 are pending. Claims 9-16 stand rejected. Claims 9, 12, 13 and 16 have been amended for formal reasons. Claim 9 has been further amended to clarify and further define patentable features that applicant regards as the present invention.

1. Applicant gratefully acknowledges Examiner's withdrawal of the 112 first paragraph rejections to the application identified on page 2 of the present office action.

2. Examiner has objected to claims 9-16 because of a typographical error in the phrase "detectable element" in claim 9. In response, Applicant has amended claim 9 to correct for this typographical error. Reconsideration and withdrawal of this objection is requested.

3. Examiner has rejected claims 12-13 under 35 USC 112 second paragraph, as indefinite for failure to provide antecedent basis for the phrase "chip card". In response, claims 12 and 13 have been amended to properly depend from claim 10, which claim provides antecedent basis for this term. Reconsideration and withdrawal of this rejection is respectfully requested.

4. Examiner has rejected claims 9-16 under 35 USC 103(a) as being unpatentable over the combination of U.S. Patent 5,499,294 ("Friedman") and U.S. Patent 6,557,104 ("Vu"). This rejection is respectfully traversed, as the proposed combination fails to teach of the features and limitations recited in present independent claims 9 and 16.

In the first instance, the Examiner states on page 4 of the present office action that "Referring to claim 9, Friedman discloses a device for authenticating the taking of pictures made up of digital data..." Examiner's assertion is incorrect as Friedman clearly fails to disclose the authentication of the taking of pictures, but instead merely authenticates the picture taking apparatus itself. This is identified in Applicant's own specification on page 1, lines 22-26, which recites

> "processes for authenticating digital images have been proposed, in particular in the patent US 5,499,294. These processes make it possible to authenticate the picture taking apparatus itself but not the journalist or cameraman." (emphasis added).

For at least this reason, Examiner's basis for rejection of present claim 9 (and of claim 16) is flawed, as the primary reference fails to teach each of the limitations asserted by the Examiner (in addition to the failings of the Friedman reference admitted by the Examiner); reconsideration and removal of this final rejection on this basis and allowance of claims 9-16 are respectfully requested.

The above notwithstanding, amended claim 9 further clarifies that the picture taking apparatus is associated with detachable security elements specific to users. In this manner, a user or group of users (e.g. a journalist or group of journalists) has a security element with a specific secret key to be authenticated as described in the specification. Present claim 9 further recites the additional limitation that the interface allows bi-directional transfer of data.

In contrast to the invention recited in present claim 9, the Friedman reference discloses a digital camera processor having a private key unique to it. Unlike the Friedman reference (and any proposed combination with Vu) the present invention comprises a picture taking device that operates with encryption keys K1 having different values where each key K is embedded in a detachable element and the camera or picture taking apparatus can work with several detachable elements. In this manner, not only are the pictures authenticated, but also the origin of the pictures (i.e. the journalist who sends the pictures).

Neither the problem nor the solution arrived at by the Applicant is disclosed or suggested by the Friedman reference, nor any of the cited references of record. Examiner attempts to improperly modify the teaching of the primary reference Friedman which teaches a "private key (which is not known to anybody except the manufacturer of the camera)" and "embedded in a probe-proof microprocessor which is itself deeply integrated into the camera's digital system" (see col. 7, lines 7-10) with that of the secondary reference Vu which teaches a "smart card that provides a secured environment for storage and processing of the secret key because all operations based on the secret key are performed within its boundary" (see col. 2, lines 11-15 and Examiner's statement on page 4 of the present office action). Even assuming arguendo, that these references can be combined, which they cannot, and that some justification exists to replace the security element embedded in the Friedman device for verifying the pictures in the camera, with the detachable security element of Vu, the Examiner's purported replacement of the security element in Friedman with the detachable

security element in Vu in order to "prevent the key from being exposed to the outside world", would nevertheless, simply move the functionality disclosed in Friedman to the detachable security element. Absent impermissible hindsight gleaned from Applicant's own invention, the detachable security element would simply perform the same processing as identified in Friedman but in the purportedly "more secured environment" of the smart card. The proposed combination still fails to teach or suggest a

> Device for authenticating the taking of pictures made up of digital data comprising a picture taking apparatus and associated with detachable security elements specific to users, each detachable security element comprising a circuit associated with a secret key K specific to that security element and carrying out the signing of at least part of the digital data to give an encrypted output digital data, the security element being connected to the picture taking apparatus through an interface allowing a bi-directional transfer of data. (emphasis added).

as recited in present claim 9.

The Vu reference relates to a method and apparatus for secure processing of cryptographic keys wherein the key is stored on a taken. Vu discloses use of a smart card having a special type of embedded integrated circuit with the smart card used as a token containing a secret key encrypted with a permanent PIN preprogrammed into an EEPROM. Furthermore, the smart card disclosed in Vu discloses the need for a specific smart card reader for allowing entry of the PIN. In addition to the arguments discussed above, there is no teaching or suggestion in Vu of such an interface circuit as recited in present claim 9 of the instant application. For at least the above

additional reasons, applicant submits that present claim 9 patentably distinguishes over any proposed combination of references and should be allowed; reconsideration and withdrawal of the 35 USC 103(a) rejection and allowance of all claims presently appearing in this application is requested.

In view of the foregoing, Applicant respectfully submits that claims 9-16 are in condition for allowance. Favorable reconsideration is requested.

If a telephone conference would be of assistance in advancing prosecution of the above-identified application, Applicants' undersigned Attorney invites the Examiner to telephone him at **609-919-4428**.

Respectfully Submitted

Date: April 19, 2004

Edward J. Howard
Registration No. 42,670
DUANE MORRIS LLP

THOMSON LICENSING INC.
Patent Operations
CN 5312
Princeton, NJ 08543-0028